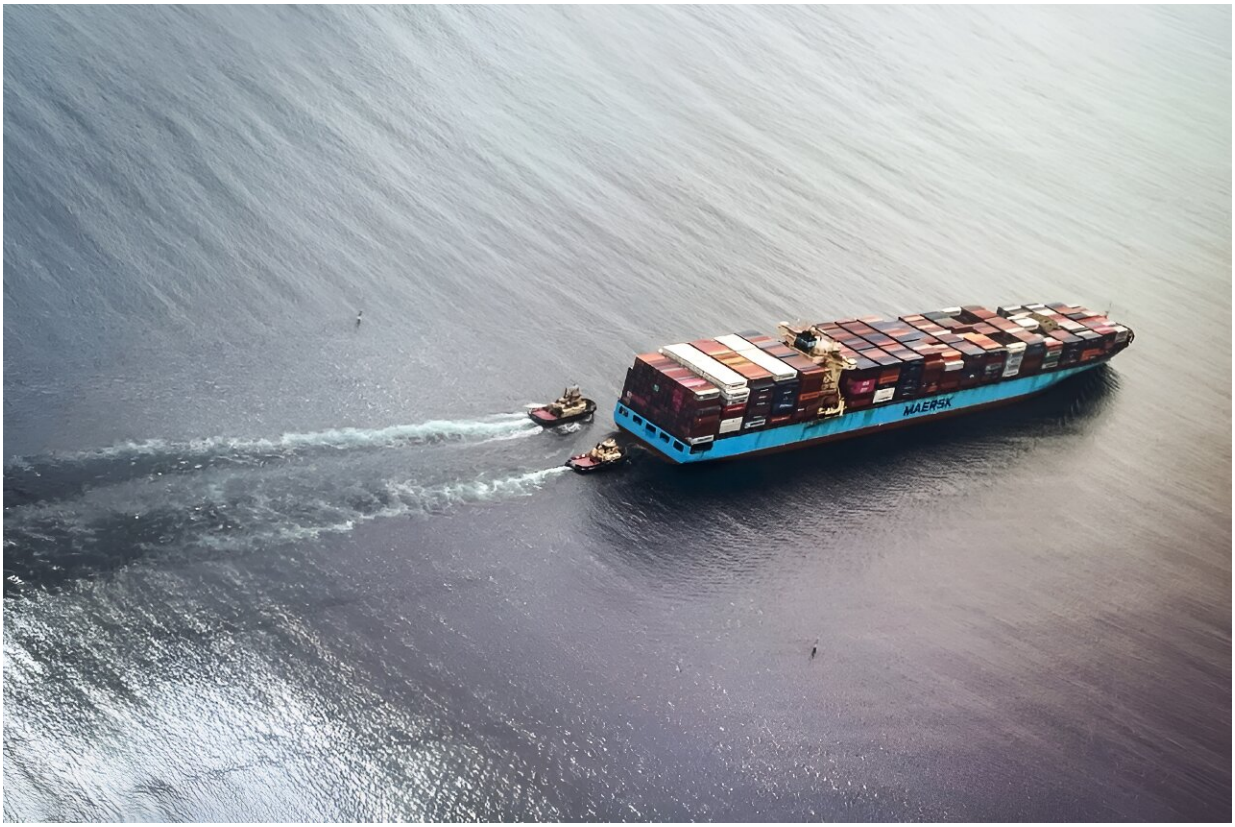
The growing cyber threat to global shipping

November 13 2023, by Qasim Nauman



A cyberattack paralyzed several major ports in Australia for days.

The cyberattack that paralyzed several major Australian ports was a sharp reminder of what governments and experts say is a growing threat to shipping, the lifeblood of the global economy.

The attack on DP World's ports—which handle 40 percent of Australia's

freight trade—forced them offline for days and was the latest in a series of breaches at ports around the world in recent years.

Who has been targeted?

Cyberattacks have disrupted or halted operations at some of the world's busiest ports in recent years.

A ransomware attack in July at Japan's busiest port, Nagoya, disrupted operations for days.

Oil terminals last year at some of western Europe's largest ports could not process vessels because of a cyberattack.

And in 2017, the "NotPetya" malware spread into systems around the world, crippling the operations of global shipping giant Maersk.

There have also been cyberattacks at major ports in the Netherlands, Canada, India, South Africa and the United States.

Nearly 75 percent of US shipping executives say their companies had faced cyberattacks, according to a 2022 survey by the law firm Jones Walker.

Why are governments worried?

Shipping is crucial to the global economy, moving more than 80 percent of trade in goods, according to the UN's trade body UNCTAD.

And the entire infrastructure contains what experts have described as single points of failure—where one cyberattack at a port can cause a logistical nightmare across the supply chain.

"If you were looking for a target, that would be the target," Rob Nicholls, an associate professor at the University of New South Wales in Sydney, told AFP.

"This is why under Australian law and increasingly around the world, ports are regarded as critical infrastructure because they are... a single point of failure in the supply chain."

The US Cyberspace Solarium Commission warned in a report this year: "A cyberattack against a complex maritime ecosystem could be devastating to the stability of the global economy."

Is shipping more vulnerable now?

Automation and connectivity in global maritime operations have increased rapidly in recent years, linking everything from cargo-handling machines at ports to traffic control in waterways to sensors on ships.

While that has boosted efficiency, security firms and government bodies have warned that there are now more points for cyberattackers to target.

An intrusion at a port manager's office, for example, could allow a hacker to insert malicious code that can in turn paralyze the entire facility.

"Ports are target-rich environments" for cyberattackers, the US research firm Mitre said in a report this year.

And the paralysis at one port could cascade around the world, said UNSW's Nicholls, offering the example of the 2021 traffic jam caused when the Suez Canal was blocked by a giant container ship.

There was "an almost universal expectation" of cyberattacks on the

shipping industry, according to an industry survey published this year by DNV, a global maritime classification and risk management firm.

"Cybersecurity is a growing safety risk," said DNV's Knut Orbeck-Nilssen, "perhaps even 'the' risk for the coming decade."